



STORMSHIELD



**STORMSHIELD ENDPOINT SECURITY
EVOLUTION**

RELEASE NOTES

Version 2

Document last updated: December 18, 2023

Reference: [ses-en-release_notes-v2.5.3](#)



Table of contents

- SES Evolution 2.5.3 new features and enhancements 3
- SES Evolution 2.5.3 fixes 7
- Compatible Microsoft Windows versions 9
- Recommendations 10
 - Updating built-in security policies and agent pools 10
 - Implementing security policies 12
 - Updating the operating system on workstations 12
- Known issues 13
- Explanations on usage 14
- Documentation resources 15
- Downloading this version 16
- Previous versions of SES Evolution v2 17
- Contact 74

In the documentation, Stormshield Endpoint Security Evolution is referred to in its short form: SES Evolution.

This document is not exhaustive and minor changes may have been included in this version.



SES Evolution 2.5.3 new features and enhancements

Warning

WARNING

Before updating your solution from a version 2.3.x to version 2.5.3, you must download and deploy the 2304a security policy. To download it, go to your MyStormshield client area or to the [Updates Stormshield](#) panel in your administration console.

Pool protection

Isolating users' computers

When there is a suspected attack on a workstation in the pool, you can now isolate the workstation from the rest of the network by cutting off incoming and outgoing connections from the administration console.

If the suspected attack is confirmed, isolating a workstation with SES Evolution can quickly prevent the attack from spreading to the rest of the pool.

In the administration console, you can isolate computers, see the list of isolated computers and undo isolation.

 [Find out more](#)

Undergo quarantine for malicious files

When creating a remediation task during an attack, you can now choose to quarantine files that you think may be malicious. These files will be placed in a protected folder on the workstation. They cannot be run or cause any harm while you analyze them, after which you can choose to restore or delete the files.

In the administration console, you can establish a list of folders to exclude. The files that they contain will never be quarantined.

You can also configure protection rules in security policies to automatically quarantine executable files.

Quarantined files are automatically deleted after 40 days or when the folder reaches 1 GB.

 [Find out more](#)

Sending e-mail notifications

SES Evolution administrators can now receive e-mail notifications when there are security alerts. You can then be quickly warned when certain events occur on your pool, without the need to constantly monitor the administration console. By using notification rules, you can configure the types of logs that trigger notifications, how frequently they are sent and the e-mail addresses of recipients.

 [Find out more](#)



Sending activity reports by e-mail

You can configure the sending of reports by e-mail. These reports provide information on the activity of your pool by recapping the security indicators and operational indicators displayed in the console dashboard. They can be sent to users who are not SES Evolution solution administrators. By using notification rules, you can configure the frequency of such reports and their language (French, English, German or Spanish).

[Find out more](#)

Protection against bypass of EDR detection (Endpoint Detection and Response) systems

In the **Threats** tab of a security policy, a new protection is available: **EDR detection bypass**. It protects against attacks that seek to disable EDR detection modules.

[Find out more](#)

Protection against fileless attacks

In the **Threats** tab of a security policy, a new protection is available: **Fileless attack**. It protects against attacks that strike without writing malicious files on workstations.

[Find out more](#)

New default policies

As of version 2307a of security policies, the default policy has been divided into three levels. There are now three default policies:

Simplified default policy	Enables the quick and simple deployment of SES Evolution in a pool by dedicating few human resources to it and without the need to modularly manage administration. Can be used without any specific configuration.
Default policy	Constitutes a balanced compromise between the need for administration and the security level matching most organizations' needs.
Hardened default policy	Raises the security level in a pool to the highest level, making administration harder. It is important that you test it with a pilot group before deploying the policy, to benefit from its policies while keeping false positives to a minimum.

New built-in rule sets

As of version 2307a of security policies, the two shared rule sets below were added.

Hardening against portable software	Blocking all executable files run outside standard installation folders.
Hardening of software installation folders	Prevents attackers from modifying a program's files in installation folders, to take their place in the system.

As of version 2310a of security policies, the two shared rule sets below were added.

EDR feature audit	This set makes it possible to launch WMI detection to search for information on updates installed on the operating systems used.
-------------------	--



Syslog - Audit template (excludes reading) to be sent to a syslog	This set is in the form of a template, making it possible to capture all events other than file reading and registry reading operations and to send them to another security solution via syslog.
---	---

Modularizing rule sets

As of version 2307a of security policies, the following rule sets have been divided so that they can be used more modularly. Features can be enabled independently without having any impact on other rule sets:

The rule set...	becomes...
Audit of attack contexts	Three rule sets: <ul style="list-style-type: none">• Audit of attack contexts• Audit of ARP spoofing protection• Audit of driver loading
Data leak prevention	Four rule sets: <ul style="list-style-type: none">• Data leak prevention - Windows• Data leak prevention - Web browsers• Data leak prevention - Vaults• Data leak prevention - Remote access tools

For further information on security policies and built-in rule sets, refer to the release notes on configuring SES Evolution security in your [MyStormshield](#) client area (under **Downloads**, then in SES Evolution **Security resources**).

SES Evolution public API

Stormshield provides a new public API that makes it possible to manage SES Evolution via orchestration solutions such as SOAR. In version 2.5.3, the public API allows you to use the following SES Evolution features, among others:

- Shut down a process;
- Delete files, keys or registry values;
- Isolate a workstation from the network;
- Perform remediation tasks during ransomware attacks. Files encrypted by the ransomware will then be restored to their initial version.

From the SES Evolution administration console, you can generate the API keys that secure access to API routes.

The SES Evolution public API is accompanied by documentation. To read the documentation, click on the link at the top right side of the **API Keys** panel in the administration console. It provides a description of API routes, the list of all parameters, and some examples.

The documentation is also available on the [Stormshield Technical Documentation](#) website.

 [Find out more](#)



Administration console

New dashboard

The dashboard in the administration console includes new key indicators that describe the status of your pool. They allow you to meet required security and operational conditions in your pool by alerting you to security events that require immediate attention.

[Find out more](#)

New layout of the main menu

The menus in the left panel, comprising the console's main menu, have been reorganized. They are now categorized under **Environment**, **Security**, **Responses** and **Backoffice**.

Stormshield resource update

When you use the Stormshield public server to download resource updates in the administration console, you can now configure and use a proxy server to contact the Stormshield server.

[Find out more](#)

Syslog server configuration

Syslog messages format

If you have chosen to send agent logs to a Syslog server, you can now add "structured data" in the header of the messages. The new **Structured data** field is available in the **Agent handlers** menu in the administration console. To know the expected data format, refer to [RFC 5424](#).

[Find out more](#)

Syslog server operational indicators

A new indicator in the upper banner of the administration console shows you the status of configured Syslog servers.

Concept of incidents replaced

The concept of "incidents" has been replaced with the concept of "contexts". By default, all Emergency and Alert logs now come with a context making it possible to thoroughly analyze the environment of attacks that occur on agents, and determine the nature, source and processes of these attacks. The attack chart is now known as the *context chart*.



SES Evolution 2.5.3 fixes

Administration console

Export incidents

Support reference: 174891PW

The feature allowing incidents to be exported no longer functioned in version 2.4.4. This issue has been fixed. In version 2.5.3, the concept of "incidents" was replaced with the concept of "contexts".

Updating the management console

Support reference: 209980CW

Following an update of the solution, the administration console occasionally could not be reopened. This issue has been fixed. However, the console may take several minutes to start the first time it is opened after the update.

Log database maintenance

Support reference: 211396CW

The manual deletion of agent logs can no longer be run while a database maintenance operation is in progress.

Display of Yara and IoC analysis logs

Yara and IoC analysis logs are now always displayed in the administration console, The log display parameter can no longer be edited when a manual or scheduled task is being created.

Management of USB device IDs

Support reference: 211108CW

Changing the **Vendor** parameter in the IDs used in a USB rule, or in the specific behavior of a USB Storage rule, could cause an automatic change to the **Product** parameter. The rule would then no longer function as expected. This issue has been fixed.

Automatic deletion of inactive agents

Support reference: 175102PW

When offline agents are automatically deleted, error logs are no longer generated in the administration console when Yara or IoC scan tasks are linked to these agents.

USB device detection

Support reference: 208241CW

If no parameters in the **Trusted devices** section are selected in the agent group configuration, USB devices connected to workstations will no longer be indicated in the management console's **Devices** menu.



Deploying the environment

Support reference: 199390CW

During the deployment of the environment over an agent pool, some requests for tiles in the administration console dashboard would fail. Error logs were displayed in System logs. This issue has been fixed.

SES Evolution agent

Use of the agent's diagnostic tool

Agents can now be updated on a workstation, repaired or have their active features modified when tracing is in progress on the workstation.



Compatible Microsoft Windows versions

Refer to the [Product life cycle](#) guide to find out more on compatibility with Microsoft Windows versions.



Recommendations

Updating built-in security policies and agent pools

Before updating an existing environment to this new version of SES Evolution:

- Read this section carefully,
- Read the section [Explanations on usage](#) carefully,
- Read the section **Known issues** in the Stormshield [Knowledge base](#) carefully (use the same login credentials as those for your [MyStormshield](#) client area).

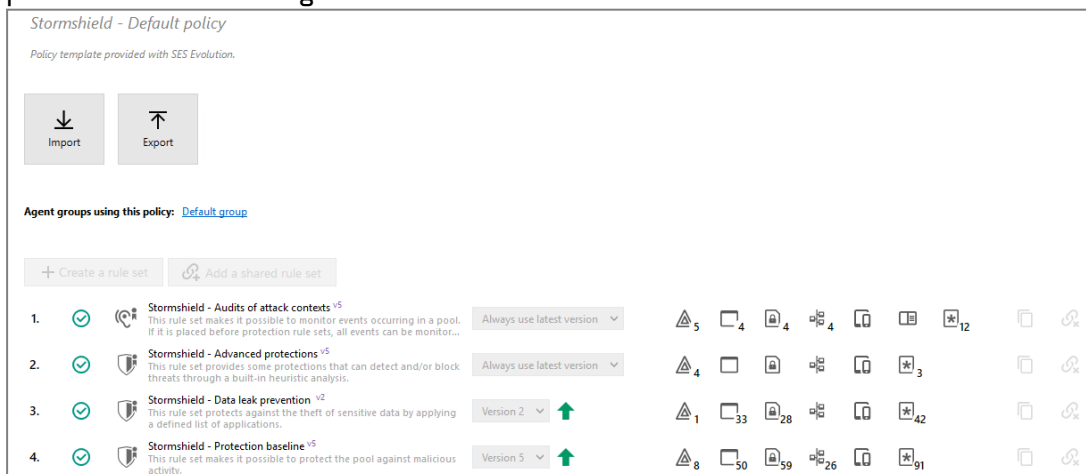
Built-in rule sets provided by Stormshield are automatically updated in the administration console when the solution is updated. However, this is not the case for built-in security policies. When necessary, you must manually update your policies in the console if any of the rule sets that they contain have a green arrow, as described in step 4 of the procedure below.

The following are the major steps involved in updating policies and the pool to this new version:

1	Updating SES Evolution via the Installation Center
2	Updating security policies to use the latest versions of rule sets
3	Creating a test agent group
4	Selecting pilot agents for the test group and monitoring their behavior for several days
5	Updating all agents to version 2.5.3

We recommend that you follow the detailed procedure below for the update:

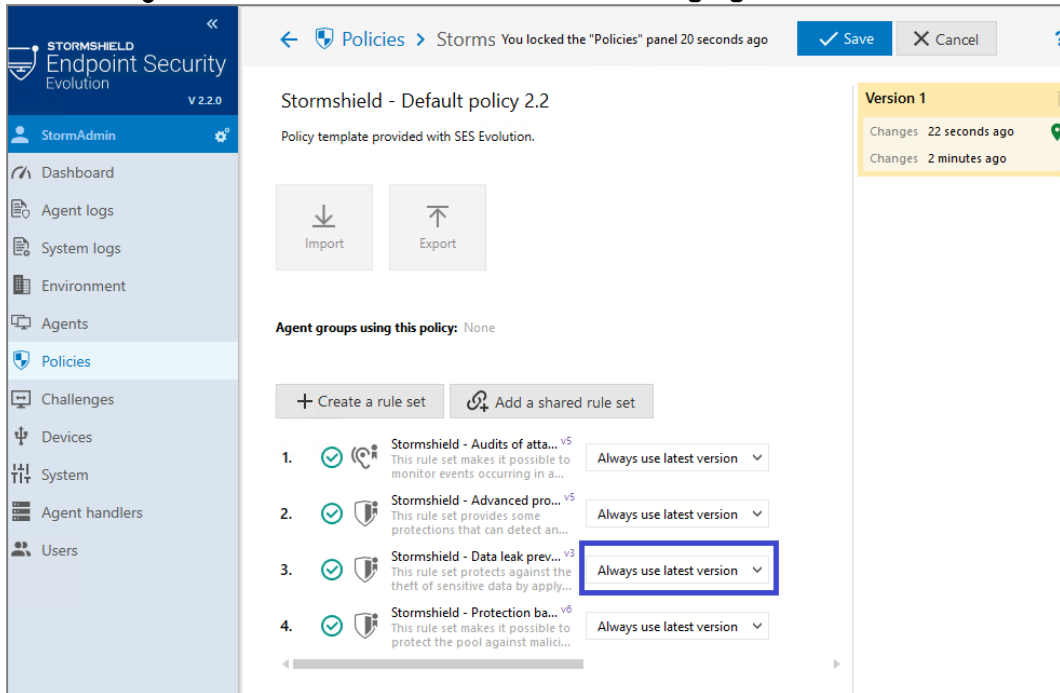
1. If there are unsaved changes in your administration consoles, save them and shut down the consoles.
2. Follow the procedure for updating SES Evolution components via the Installation Center, as explained in the [Installation guide](#).
3. Once the update via the Installation Center is complete, open the consoles again to finalize the update. A message will warn you that the security policies are not using the latest version of the rule sets. Policies were not automatically updated in order to prevent compatibility issues with agents in versions lower than version 2.5.3.
4. Select a console. In the **Security > Policies** menu, a green arrow pointing upwards indicates policies that are not using the latest version of some rule sets.



Duplicate a policy containing a green arrow, such as the default policy, for example.



5. Select the copy of the policy and click on **Edit**.
6. Rename the policy by adding the version number "2.5.3" for example.
7. Select **Always use latest version** for all rule sets containing a green arrow.



8. Save the policy.
9. In the **Environment > Agents** menu, duplicate one of your production agent groups to test the deployment in version 2.5.3 with the new updated policy.
10. In the **Policies** tab, select the policy created earlier.
11. Ensure that the software version selected in the **Version** section of the **Settings** tab is 2.5.3.
12. Save the new group.
13. You will now select one or several agents in your initial group, which will be used as pilot agents. In the **Agents** tab of the initial group, select the pilot agents and click on **Move agents to**. Select the new test group.
14. In the **Security > Deployment** menu, click on **Deploy** to deploy the changes made to your environment.
15. After the pilot agents have reconnected to the agent handler, the workstations must be restarted. After restarting, ensure that the agents have indeed switched to software version 2.5.3 and that they are using the new policy.

Test the behavior of the pilot agents for several days. Once you are sure that they are running properly, you can update all the agents in the pool. There are two ways to do so:

- Select the new policy and software version 2.5.3 in your production agent groups. If you choose this option, remember to delete the test group.

- or -

- Duplicate all your production groups and update them, then delete older groups if necessary.

If there is a need for agents to downgrade to an earlier version after updating to version 2.5.3, the version would no longer be compatible with the policies that contain version 2.5.3 features. We recommend that you then move the affected agents back to their original group.



Implementing security policies

With version 2.5.3, Stormshield provides version 2310b of the security configuration. This is the default configuration and includes policies as well as protection rule sets and shared audit rule sets. You can use these rule sets in your own policies.

You can refer to the release notes regarding version 2310b of the security configuration by going to **Downloads** in your [MyStormshield](#) client area, then SES Evolution **Security resources**.

To build your policies, you can follow the recommendations mentioned in the release notes on the security configuration relating to the order of sets and the sets to use in your policies.

For more information, refer to the sections [Understanding built-in rule sets](#) and [Customizing built-in rule sets](#) in the SES Evolution *Administration guide*.

Updating the operating system on workstations

Before updating the Microsoft operating system on workstations that host SES Evolution agents, ensure that you have the most recent Stormshield rule sets. If this is not the case, download the latest rule sets as described in the section [Downloading Stormshield updates](#) in the *Administration guide*, then update your security policies.



Known issues

The up-to-date list of the known issues related to this version of SES Evolution is available on the [Knowledge Base](#) Stormshield. To connect to the Knowledge base, use the same identifiers as for [MyStormshield](#).



Explanations on usage

Using the Sysprep tool in Windows Server 2019

If you need to use the Microsoft Sysprep tool on a workstation that runs in Windows Server 2019, we recommend that you apply a blank security policy beforehand to prevent a blue screen. Once you have restarted the workstation, you can apply the nominal security policy again.

Controlling access to files and copying files

When files are being copied on a network share, file access rules will not apply if the source and destination files are in the same share. However, they will apply when a share is copied to the local host, or shared on another share.

Compatibility with Windows Smart Application Control protection

From version 2.4 onwards, SES Evolution is compatible with Smart Application Control protection, which is available with a fresh Windows 11 22H2 installation (disabled by default). However, when the agent is installed, informational warning messages will be generated regarding drivers that the agent runs.

SES Evolution online help

The version of the online help accessible from the administration console is always the latest available version, regardless of the console version installed.

Challenges

On a console from version 2.4, the challenge mechanism cannot be used with agents in version 2.3.x and below.

Protection against WMI Persistence

Advanced protection against WMI persistence is incompatible with the 32-bit and 64-bit versions of the Microsoft Windows 10 LTSB 2015 operating system. Even if it is enabled, it will not run on this operating system. However, this incompatibility does not prevent the SES Evolution agent from functioning normally.

SES Evolution installation

If a Windows update is in progress during a full installation of SES Evolution server or of the backend component, the installation will fail. It is recommended to disable Windows update before installing SES Evolution, and to enable it again afterwards.

Bluetooth Low Energy devices

The SES Evolution agent does not filter Bluetooth Low Energy devices; only standard Bluetooth devices are recognized.



Documentation resources

The following technical documentation resources are available on the [Stormshield Technical Documentation](#) website or on Stormshield [Institute](#) website. We suggest that you rely on these resources for a better application of all features in this version.

Guides

- [Installation guide](#)
- [Administration guide](#)
- [SQL Server Recommendations guide](#)
- [Public API documentation](#)

Please refer to the [Knowledge Base](#) for specific technical information.



Downloading this version

Going to your MyStormshield personal area

You need to go to your [MyStormshield](#) personal area in order to download the 2.5.3 version of Stormshield Endpoint Security Evolution:

1. Log in to MyStormshield with your personal identifiers.
2. In the left panel, select **Downloads**.
3. In the right panel, select the relevant product and version.

Checking the integrity of the binary files

To check the integrity of Stormshield Endpoint Security Evolution binary files:

1. Enter one of the following commands and replace `filename` by the name of the file you want to check:
 - Linux operating system: `sha256sum filename`
 - Windows operating system: `CertUtil -hashfile filename SHA256`
2. Compare with hashes provided on [MyStormshield](#) personal area, section **Downloads**.



Previous versions of SES Evolution v2

In this section, you will find the features and fixes from previous versions of SES Evolution v2.

2.5.0	New features		
2.4.5			Bug fixes
2.4.4			Bug fixes
2.4.3		Resolved vulnerabilities	Bug fixes
2.4.2			Bug fixes
2.4.1	New features	Resolved vulnerabilities	Bug fixes
2.3.2	New features		Bug fixes
2.3.1	New features		Bug fixes
2.2.3	New features		Bug fixes
2.2.2	New features		Bug fixes
2.1.2		Resolved vulnerabilities	
2.1.1			Bug fixes
2.1	New features	Resolved vulnerabilities	Bug fixes
2.0.2			Bug fixes
2.0.1		Resolved vulnerabilities	Bug fixes
2.0.0	New features		



Version 2.5.2 SaaS mode

SES Evolution version 2.5.2 is only available in SaaS mode.



Version 2.5.1 SaaS mode

SES Evolution version 2.5.1 is only available in SaaS mode.



SES Evolution 2.5.0 new features and enhancements

SES Evolution as a Service (SaaS)

SES Evolution is now available as a Service. This means you can benefit from SES Evolution protection with appropriate security policies, without having to install an administration server in your infrastructure. Configuring, administering and monitoring the solution can now be performed remotely in the cloud by a managed security service provider (MSSP). The SES Evolution is the only component to be deployed on the workstations.

SES Evolution version 2.5.0 is only available in SaaS mode.



SES Evolution 2.4.5 fixes

Warning

WARNING

Before updating your solution from a version 2.3.x to version 2.4.5, you must download and deploy the 2304a security policy. To download it, go to your MyStormshield client area or to the [Updates Stormshield](#) panel in your administration console.

Administration console

Management of the log database size

Support references: 211151CW, 211647CW

If a very large number of logs were issued, they could quickly saturate the log database. To avoid this problem, a degraded mode is now enabled when the log database reaches 81% of its maximum size. While this mode is active, a red warning banner displays in the lower part of the administration console.

New agent and system logs sent to the Backoffice are no longer stored in the log database, but are permanently deleted.

However, if you have configured Syslog servers for agent managers, they will continue to receive agent logs.

To disable this degraded mode, click on the **Back to standard mode** button. This operation can only be performed if the log database volume is below the 81% threshold. You must therefore previously adjust your security policy and [manually delete agent logs](#).



SES Evolution 2.4.4 fixes

Warning

! WARNING

Before updating your solution from a version 2.3.x to version 2.4.4, you must download and deploy the 2304a security policy. To download it, go to your MyStormshield client area or to the [Updates Stormshield](#) panel in your administration console.

Administration console

File access control rules

After the latest versions of Windows 10 and 11 were installed, read and write file access rules were not applied when files were copied.

This issue appeared with the following Windows updates:

- Windows 10 20H2 build 19042.2788, KB5023773 [21/03/2023]
- Windows 10 21H2 build 19044.3086, KB5027215 [13/06/2023]
- Windows 10 22H2 build 19045.2913, KB5025297 [25/04/2023]
- Windows 11 21H2 build 22000.1761, KB5023774 [28/03/2023]
- Windows 11 22H2 build 22621.1105, KB5022303 [10/01/2023]

The issue has since been fixed, except for a limitation on network shares, described in the section [Explanations on usage](#).

Export incidents

Support reference: 207668CW

The export path selection window now appears immediately after clicking on the **Export incidents** menu.

Agent logs display

In the Agent logs panel, the rule description is now correctly displayed in logs regarding security rules.

Deleting IoC or Yara resources

IoC or Yara resources that are linked to an already deleted agent can now be deleted.

IoC search logs

The log settings specified when an IoC scan task is created are now correctly applied.

Helpdesk role

Users with the Helpdesk role can now open the administration console and change its language.



SES Evolution agent

Windows event forwarding

Support reference: 209227CW

In the administration console, SES Evolution agents now systematically report all items detected by Windows event forwarding rules.

DNS request processing

Support reference: 208562CW

In some rare cases, the agent would wrongly interpret DNS requests sent by applications. This would cause the applications in question to malfunction. This issue has been fixed.

Backoffice components

Collecting data from databases

Support reference: 208562CW

The task of collecting diagnostic data in databases no longer fails when an SES Evolution update is run at the same time, or if it is not complete.

Sending agent logs to a Syslog server

The brief description of agent logs, which appears in the administration console, is now forwarded to Syslog servers in JSON format.



Resolved vulnerabilities for SES Evolution 2.4.3

SES Evolution agent

Two low severity vulnerabilities were fixed.

Details on these vulnerabilities can be found on our website:

- <https://advisories.stormshield.eu/2023-021/>
- <https://advisories.stormshield.eu/2023-022/>



SES Evolution 2.4.3 fixes

Warning

! WARNING

Before updating your solution from a version 2.3.x to version 2.4.3, you must download and deploy the 2304a security policy. To download it, go to your MyStormshield client area or to the [Stormshield updates](#) panel of the administration console.

Administration console

Agent log details

In some cases, the administration console would stop unexpectedly when displaying the details of an agent log. This issue has been fixed.

Syslog server

Logs in JSON format

The agent IP address was not included in the agent logs in JSON format sent to the Syslog server. This issue has been fixed.



SES Evolution 2.4.2 fixes

Warning

! WARNING

Before updating your solution to version 2.4.2, download and deploy the 2304a security policy. To download it, go to your MyStormshield client area or to the [Updates Stormshield](#) panel in your administration console.

SES Evolution agent

Compatibility between the SES Evolution agent and the Microsoft Windows operating systems

The signature process of SES Evolution drivers has been reviewed in order to maintain the compatibility with Windows 7, Windows 8.1, Windows Server 2008 R2 and Windows Server 2012 R2 operating systems.



SES Evolution 2.4.1 new features and enhancements

Warning

WARNING

Before updating your solution to version 2.4.1, download and deploy the 2304a security policy. To download it, go to your MyStormshield client area or to the [Stormshield updates](#) panel of the administration console.

Improved pool protection

Integrated search for indicators of compromise

SES Evolution now makes it possible to search for Indicators of Compromise (IoC) on your entire pool or part of it. IoCs are able to detect attacks on a user workstation, prevent their spread and clean up systems before a compromise is exploited.

Indicators may be, for example, file names, specific IP addresses, malicious file hashes, suspicious URLs or text files.

IoC searches can be launched when a security rule detects or blocks abnormal behavior. Searches can also be launched manually at any time to monitor one or several workstations on demand. You can also schedule IoC scans by agent group, at regular intervals and for a specified duration.

To search for IoCs, you must first provide SES Evolution with the IoC description. IoCs may originate from your own pool if you have detected a compromise via SES Evolution or other means, or from external private or public resources.

 [Find out more](#)

Remediation operations on a group of workstations

In an attack or malicious operation on your pool, you can now launch remediation operations on several workstations from agent logs generated in the administration console. These operations make it possible to limit the impact of attacks and fix any damage caused.

Depending on the agent log type, SES Evolution offers various remediation operations, for example: deleting a file or registry key, shutting down a process or retrieving files encrypted by ransomware

 [Find out more](#)

Detection of Windows Store apps

SES Evolution can now detect app signatures that have been validated by Microsoft to be distributed via Windows Store. This verification makes it possible to extend the verification of legitimate apps to Windows Store apps and rely on the analysis of information contained in apps' certificates.



Database management

Monitoring of administration and log databases

With the calculation of estimates and alerts, SES Evolution now allows users to monitor the remaining capacity in databases and prevent them from being saturated. In the **System** menu of the administration console, charts provide a quick overview of database occupation and make it possible to estimate when they will be saturated.

To anticipate when databases will be saturated so that they can be reduced, SES Evolution allows you to:

- Schedule daily maintenance tasks to optimize database performance,
- Manually delete logs immediately,
- Schedule when logs older than a certain date will be automatically deleted.

In addition, SES Evolution now makes it possible to export incidents that are reported in the event of an attack. You can then submit them to an external service for analysis, for example, and archive them as well on a storage server to free up space on the log database.

 [Find out more](#)

Troubleshooting

Diagnostic tool

When abnormal incidents occur, the new SES Evolution diagnostic tool collects data about the component causing the issue (agent and backoffice) and the host's Windows system. Stormshield's technical support team can then analyze this data to form a diagnosis.

 [Find out more](#)

Administration console

New shortcut icons

In the administration console, a new banner at the top of the window shows several icons with direct access to menus in the console:

- Three icons indicating the status of the backend server, databases and agent handlers. Click on each icon for more details.
- An icon to access the **Environment** menu. When a deployment is required, the icon will turn red.
- An icon to access user preferences.
- An icon to access the **Stormshield updates** menu.

SES Evolution Agent

Compatibility with Smart Application Control

The SES Evolution agent is now compatible with the Smart Application Control option on Windows 11 22H2 operating systems. We advise you to refer to the section [Explanations on usage](#) for more information.



Security policies

Wi-Fi network rules

The WPA3 authentication mode is now available in the Wi-Fi network rules in security policies to allow such connections to be blocked, allowed or monitored.

 [Find out more](#)

Compatible SQL Server versions

New compatibility

SES Evolution is now compatible with SQL Server 2022 and SQL Server Express 2022 databases.



Resolved vulnerabilities for SES Evolution 2.4.1

Backend

Two low severity vulnerabilities were fixed.

Details on these vulnerabilities can be found on our website:

- <https://advisories.stormshield.eu/2023-001/>
- <https://advisories.stormshield.eu/2023-002/>



SES Evolution 2.4.1 fixes

SES Evolution agent

Agent integrity verification

Support reference: 199381CW

The agent integrity verification has been optimized and the severity of logs generated by this verification has been reviewed to make it more consistent with the severity of the reported information.

Outbound UDP connections

Support reference: 192545CW

The SES Evolution application firewall now optimizes the processing of outbound UDP connections on the user's workstation so that it no longer slows down the transmission of certain network packet types or disrupts the operation of third-party apps.

Administration console

Simultaneous use of multiple consoles

The stability of the SES Evolution backend server has been enhanced to support the simultaneous use of multiple administration consoles.

Operations on devices

All operations performed in the console's **Devices** menu are now logged in System logs: when keys are added, modified, deleted, etc. In addition, the list of vendors and USB devices in security policies has been updated.

Automatic creation of application IDs

Support reference: 172154PW

When you add an exception to a log that was generated by the activation of the advanced protections **Environment discovery** or **Malicious use of certutil**, the ID created automatically in the exception rule now includes the children of the app identified.

Name of the Command line criterion in application IDs

Support reference: 172856PW

When a Command line criterion is added in application IDs, the **Show more** link remains displayed in the main panel of the ID, even when the criterion is very long.

Challenges

Support reference: 201634CW

An issue regarding the operation of the challenge mechanism has been fixed.



Importing custom rule sets

Support reference: 201083CW

When rule sets are imported into a security policy, shared rule sets can no longer be overwritten with private rule sets, unless you have deleted the shared sets from the console.

When rule sets are deleted, they remain in the database. As a result, if you import a custom rule set that has the same ID as a deleted rule set, the version number of the imported set will be incremented by one from the version of the deleted set.

Deleting shared rule sets

Support reference: 201151CW

Deleted shared rule sets can now be restored, by restoring a version or revision of a policy that contained such sets.

Environment discovery protection

Support reference: 172473PW

The **Environment discovery** protection has been improved to reduce the number of false positives.

Database overloaded when incident context logs fail to be inserted

Support reference: 205490CW

When an agent generates simple context logs during an incident, if the insertion of such logs into a database fails, any new attempts by the agent handler to insert them will now be restricted for the first few days. After nine days, no more attempts will be made. A system log will then warn the user that context logs have been deleted. This fix makes it possible to avoid overloading the database with logs.



Version 2.4.0 not published

Version 2.4.0 is not available to the public.



SES Evolution 2.3.2 new features and enhancements

SES Evolution Agent

Uninstalling the SES Evolution agent

With the new *AgentRemovalTool.exe* tool available in your [MyStormshield](#) client area, SES Evolution agents can be uninstalled when a standard uninstallation is not possible. This tool runs in Windows safe mode and is compatible with all versions of the agent. It will be updated regularly so that it stays compatible.

[Find out more](#)



SES Evolution 2.3.2 fixes

Installation Center

Improvements to the demo installation

During the configuration of authentication settings in the demo installation, the Installation Center would occasionally generate an error. This issue has been fixed.

SES Evolution Agent

Plugging the USB device into a decontamination station

In some cases, the highest trust level could not be granted to USB devices plugged into a decontamination station due to an issue with access privileges. This issue has been fixed.

Integrity check and agent repair

The agent integrity check and agent repair functions via EsaUpdateSvc have been improved. Agent repair is now launched only when necessary.

Support reference: 199298CW

Compatibility with device control applications

Compatibility with third-party device control applications has been improved for agent installations and updates.

Support reference: 197055CW

Stopping agent processes

When processes that enable interaction with the SES Evolution agent (e.g., *EsSetup.exe* and *EsGui.exe*) stop running, the logs generated as a result now include the 'Notice' severity level. Previously, they indicated the 'Error' level.

Support references: 197090CW, 197091CW and 197092CW

Agent self-protection

The self-protection of the agent interface has been greatly improved. It is highly recommended to install this new version.

Administration console

Downloading policies from the Stormshield public update server

Built-in security policies on the Stormshield public update server can now be downloaded again and installed in the administration console, even if they had already been installed before and removed from the console.



Communication between the console and the backend server

Support reference: 199390CW

The maximum response time is now longer when the administration console sends requests to the backend server. The purpose of this extension is to prevent false error logs from being generated, and reduce the volume of system logs.

Installation Center and administration console

Keep logs forever option

The **Keep logs forever** option can now be selected again in the Installation Center and the **System** tab in the administration console.. This option is available only when SQL Server Enterprise is used.

Third-party libraries

Yara library update

The Yara library used by Stormshield has been updated to version 4.2.3, as this version resolves a vulnerability.



SES Evolution 2.3.1 new features and enhancements

Improved pool protection

Built-in Yara scan tool

SES Evolution now integrates the Yara scan tool, which is based on rules that make it possible to detect binary or textual patterns in files or running processes. By recognizing known patterns, Yara identifies threats or attacks targeting workstations. The administrator can then set up remediation actions.


Yara scans can be launched when a security rule detects or blocks abnormal traffic, but you can also launch Yara scans manually at any time, to monitor one or several agents on demand. These scans can also be scheduled by agent group, at regular intervals and for a specified duration.

Yara is an open-source tool with free online documentation that explains how to build rules. Depending on the current events, Stormshield will also provide Yara rules in order to detect potential new threats.

 [Find out more](#)

Stormshield resources

Automatic updates of policies and rule sets

When a new version of SES Evolution is installed, it contains the most recent versions of built-in security policies and built-in rule sets. However, Stormshield may sometimes publish an update of any of these resources separately from a version to provide a quick antidote to new threats or a quick reaction to changes in third-party products. You can now easily access these updates from the console and choose to install them automatically. The  icon allows you to access the new panel from which resources can be downloaded.

Resources are available by default on the Stormshield public server. You can also configure a local server of your choice if you work in an offline environment.

Detailed descriptions are given of the changes made in the new versions of policies and rule sets. These descriptions are available only in French and English.

 [Find out more](#)

New protections

Parent PID Spoofing protection

The new protection against parent PID spoofing is available in the **Threats** tab of a protection rule set. It prevents hackers from starting programs that they would declare as children of arbitrarily chosen existing processes.

New shared rule sets II 901

The following rule sets have been added to the shared rule sets in the administration console. With these rules, sensitive information systems can be protected, in line with the French



interministerial instruction no. 901 drafted by the ANSSI. These five rule sets are templates. To use them, adapt them to your environment by duplicating them in your policies.

II901 - Common application hardening template

II901 - Common device hardening template

II901 - Network client hardening template

II901 - Network server hardening template

II901 - USB decontamination station hardening template

In addition, the new shared rule sets below can be downloaded from your [MyStormshield](#) personal area or from the Stormshield public server:

Protection against malicious usage of LOLBIN	This protection set prevents hackers from using certain Microsoft LOLBIN binary files maliciously.
Block-list of known dangerous applications	This protection set blocks the startup of known harmful applications identified by hash or by certificate
Monitoring of known dangerous or vulnerable drivers	This audit rule set raises alerts when a known dangerous or vulnerable driver is loaded.

[Find out more](#)

Changes to existing rule sets

Some existing built-in rule sets have been modified. SES Evolution2.5.3 includes v2.3.2.2208a rule sets.

For details on these modifications, refer to *Stormshield rule sets release notes* in the **Downloads** menu in your [Mystormshield](#) personal area.

Refer to [Recommendations](#) to find out our recommendations with regard to implementing security policies.

Activity monitoring

Grouping of similar logs

When similar events occur on one or several agents, the generated logs are now displayed by group in the **Agent logs** menu of the administration console. In this way, there are considerably fewer lines of logs to read, and grouped logs can be easily distinguished from isolated logs. Many details are shown in log groupings, such as the dates and times of the first and last logs.

You can also add exceptions for all logs in a grouping by applying a single action.

[Find out more](#)

Google and VirusTotal search links from agent logs

In the details of an agent-generated log, which can be accessed from the **Agent Logs** menu of the administration console, two new links make it possible to check the maliciousness of each process involved, either on [Google](#) or the [VirusTotal](#) website.

[Find out more](#)



New information in system logs

System logs now indicate all changes made in the administration console with regard to agent groups and agent handlers.

Compatible Microsoft Windows versions

New compatibilities

SES Evolution now supports Windows Server Core 2012 R2, 2016, 2019 and 2022 operating systems for all its components except the administration console.

Security policies

Enabling Detection mode on policies and rule sets

SES Evolution now offers Detection mode for security policies and rule sets. When this mode is enabled, agents do not block operations, but instead, generate logs indicating the operations that would have been blocked by a rule. This allows you to easily test security policies or rule sets on a pool before using them in a production environment and without disrupting users, so that you can measure the impact of restrictions and make adjustments accordingly.

You can enable Detection mode on an entire policy in the agent group settings, or on individual rule sets in a policy.

 [Find out more](#)

Removable Devices

Filtering USB devices at startup

Security rules that make it possible to monitor the use of USB devices now apply as soon as a workstation starts up, before the Windows session opens.

 [Find out more](#)

Administration console

Contextual help

Context-relevant sections of the SES Evolution solution documentation can now be accessed from the panels in the administration console.

Versions of rule sets and advanced protections

When a policy uses rule sets or advanced protections that are not in their most recent versions, a new visual indicator now appears in the console. A button on the row of such a rule set makes it possible to easily update the set.

 [Find out more](#)

Using the dashboard

You can now browse from the dashboard to the various panels of the console by using several links spread out over graphs, icons and text segments in the dashboard.

 [Find out more](#)



Copying and pasting rules

Rules can be copied and pasted between rule sets of the same type (audit or protection) and between policies.

Duplicating agent groups

Existing agent groups can be duplicated in the administration console to create a new group. While the duplicated group keeps all the settings of the original group, it does not contain any agents.



SES Evolution 2.3.1 fixes

Installation center

Lowest SQL Server version

The Installation center now refuses to install or update SES Evolution if your version of SQL Server is lower than the minimum version required, i.e., SQL Server 2017 Cumulative Update 25 [14.0.3401.7].

Administration console

Connecting with the backend

Support reference: 194069CW

The configuration of the administration console has been modified to keep and reuse TCP connections as much as possible. This somewhat reduces network traffic and latency on the console.

SES Evolution agents

Agent interface display

The commands *EsGui.exe* and *EsGui.exe /ShowPanel* now correctly display the agent's interface, even when it has already been launched but is not visible.

Agent export file

Support reference: 167578PW

The process of exporting information about agents in a .csv file has been improved in the administration console:

- The file contains column titles to make reading easier,
- The columns in the .csv file correspond to the information that can be seen in the list of agents in the administration console,
- The type of separator can be selected (comma, semicolon or tab).

Security policies

Protection against privilege escalation

Support reference: 192169CW

The mechanism that protects against privilege escalation no longer generates logs when a user without administration privileges attempts to uninstall an application.



Rule set version

After a deployment, a rule set always shows which version of the set was deployed. However, in "edit" mode, rule sets that have been configured to **Always use latest version** now keep this setting and no longer show the version deployed.

Agent logs

Application filter

Support reference: 189842CW

The **Application** filter in agent logs has been split into two filters: **Application** and **Target application**, to differentiate applications that performed an action from those on which the action was applied.

Getting agent logs

Support reference: 193939CW

Requests to get agent logs have been improved to shorten the display time in the administration console.

Adding an exception for a log triggered by a file access rule

Support reference: 197182CW

Creating an exception rule from some logs triggered by a rule controlling access to files no longer causes error while applying the security policy after a new deployment on agents.

USB storage devices

Display in the administration console

Support references: 192880CW - 193078CW

When a USB device is plugged into an agent and its enrollment fails, it now appears in the SES Evolution administration console. Its trust level is 0.

Logs relating to USB devices

Support reference: 183857CW

When information about the name of the vendor and the name of the product is missing, it no longer appears with the value <NULL> in SES Evolution. It has since been replaced with the vendor ID and product ID.



Version 2.3.0 not published

Version 2.3.0 is not available to the public.



SES Evolution 2.2.3 new features and enhancements

Agents

Tracing via a script

When an issue occurs on a workstation, tracing can now be launched via a script, by running EsGui ([...]\Stormshield\SES Evolution\Agent\Bin\Gui) with the command line option /StartDiagnostic.

You can indicate the name of the final log file: EsGui.exe /StartDiagnostic /DiagnosticFile <path\to\file.cab>.

You can also stop tracing: EsGui.exe /StopDiagnostic.

[Find out more](#)

Deploying agents via a group policy

In your [MyStormshield](#) client area, Stormshield now provides a PowerShell script that allows you to deploy SES Evolution agents in a pool, by using a group policy (GPO). You can find it under Downloads > Stormshield Endpoint Security > Evolution > Tools.

[Find out more](#)

Changes to existing rule sets

Some existing built-in rule sets have been modified. SES Evolution2 includes rule sets v2.2.3.2204a.

For details on these modifications, refer to *Stormshield rule sets release notes* in the **Downloads** menu in your [MyStormshield](#) personal area.

Refer to [Recommendations](#) to find out our recommendations with regard to implementing security policies.



SES Evolution 2.2.3 fixes

Compatibility with third-party products

Compatibility with Windows Sandbox

Support reference: 192983CW

A compatibility issue between SES Evolution and Windows Sandbox that occasionally caused a blue screen of death (BSOD) has been fixed.

Logs

Reduced severity

Support reference: 189040CW

SES Evolution generates logs whenever backoffice components access a known registry key to allow DLL injection. The severity of such logs has been lowered from “Notice” to “Informational” level.

Agent update or repair

Support reference: 168746PW

In the agent’s interface, the log indicating that an agent update or repair was successfully completed has been changed to inform the user that the agent must be restarted to finalize the operation.

SES Evolution agents

Workstation at startup

Support reference: 191475CW

The SES Evolution processes *EsaRulesEngDrv* and *EsaKrnlCtrlDrv* no longer cause a blue screen of death (BSOD) when some workstations start running.

Edition of the agent ID

The *EsSetup.exe* executable file now accepts the “/newagentid” or “-newagentid” option as a way to abandon the unique ID of the agent that is already installed. A new unique ID will then be assigned to the agent when it retrieves a new communication certificate from an agent handler.

Agent update

In some cases, the workstation may take longer to start up. The execution of the agent’s various services has been optimized to shorten the wait.



Downgrading to an older version

To allow downgrades to an older version of the agent when issues occur, changes have been made in version 2.2.3 so that downgrading remains possible from future versions of SES Evolution.

Unblocking the agent

Support reference: 192599CW

The self-protection system on agents has been improved so that agents that are not connected and have a highly restrictive security policy can be unblocked.

USB devices

Viewing USB devices in the console

Support reference: 193035CW

Whenever a USB device was manually deleted from the administration console but not unplugged from the workstation, the device would continue to appear in the list when the user unplugged the device. This issue has been fixed.

USB devices deleted from the console will appear in the console once again the next time they are inserted.



SES Evolution 2.2.2 new features

New protections

Anti-ransomware protection

SES Evolution 2.2.2 now protects your organization's workstations from ransomware attacks. It can detect operations that ransomware applications usually perform on a system and quickly stop them.

SES Evolution has provided a new "Anti-ransomware protection" rule set for this purpose. This rule set is available in shared rule sets, and is included in the Default policy. An anti-ransomware protection rule also appears in the **Threats** tab of rule sets.

If the ransomware manages to modify or encrypt files before the attack can be blocked, SES Evolution will provide a list of such files to help you restore them. For the same purpose, SES Evolution now also offers a mechanism that creates and protects shadow copies (also known as snapshots) in Windows, as described in the following section.

 [Find out more](#)

Shadow copy protection in Windows

Microsoft Windows offers a data backup mechanism with which shadow copies or snapshots of a workstation's local NTFS volumes can be created. These shadow copies make it possible to restore lost data.

SES Evolution now detects and blocks the deletion or corruption of shadow copies on workstations. Such malicious operations are usually among the first that ransomware applications execute.

Saving Windows shadow copies

SES Evolution also allows you to save shadow copies for your entire pool. Each SES Evolution agent will then create a shadow copy per day for every local NTFS volume on protected workstations. The last five copies will be kept.

To use this feature, you must first allow the creation of shadow copies for all NTFS volumes on the workstations and ensure that they have sufficient reserved disk space.

 [Find out more](#)

Updating the Default policy

The Default policy has been enriched with the addition of an anti-ransomware protection rule set.

When updating from SES Evolution 2.1.x to version 2.2, refer to the [Recommendations](#) to find out the steps to take with regard to policy updates.

 [Find out more](#)

New built-in rule sets

In addition to the "Anti-ransomware protection" rule set, the two shared rule sets below were also added. Prior to SES Evolution 2.2.2, the rules that made up these sets were found in the "Protection baseline" rule set, which was part of the Default policy. They were removed from the Protection baseline set to form independent sets that are available in the shared sets.



Common applications hardening	The set provides better control over how common applications behave, which may sometimes be dangerous, even if the source is not malicious.
Common network hardening	The set provides better control over applications that may generate unwanted network traffic.

 [Find out more](#)

Changes to existing rule sets

Two existing built-in rule sets have been modified and enriched. For details on these modifications, refer to the *Stormshield rule sets release notes* in your [MyStormshield](#) personal area.

Refer to [Recommendations](#) to find out our recommendations with regard to implementing security policies.

Compatible Microsoft Windows versions

New compatibilities

SES Evolution now supports Windows 10 21H2, Windows 11 and Windows Server 2022 operating systems.

Application identifiers

Filtering applications and processes via command line arguments

Some applications can be used on your appliance pool by your administrators for legitimate purposes, but can also be used maliciously by attackers.

For better control over the use of applications, SES Evolution now makes it possible to filter their operations more granularly based on the settings of their command line. These settings can be specified as criteria in application IDs, making it possible to apply different rules to the same application, depending on how it is used. For example, you can prevent PowerShell from running only when it is run as a hidden process, or when its command line parameters attempt to bypass Windows execution policies.

 [Find out more](#)

Configuration deployment

Deployment indicator

The SES Evolution console now shows a visual indicator opposite the **Environment** menu, showing that you have modified the configuration and that it must be deployed in the agent pool.

 [Find out more](#)



Activity monitoring

Browsing between logs and exception rules

In the agent logs panel of the administration console, a new button leads you directly to exception rules created from a log, if you need to read or modify them.

Server configuration

Disk space monitoring

In the SES Evolution console, the dashboard now indicates the disk space used on the servers that host backends, agent handlers and databases. You will be warned when any thresholds are reached. Monitoring disk space allows you to anticipate disk space issues and guarantee service continuity.

 [Find out more](#)



Administration console

New features have been added to the administration console to facilitate the management of policies and rules:

- If you wish to export policies or rule sets, you can now choose which items to export. They will then be exported in separate files.
- The number of existing rules is now shown on each tab of the various rule types in a set.
- When you select shared rule sets to add to a policy, they are now added in the order of selection.
- Rules can now be copied/pasted or cut/pasted within the same rule set.

Icon of the agent on workstations

Icon changed in the taskbar

On workstations, the old icon  of the agent has been replaced with the icon  in the taskbar.



SES Evolution 2.2.2 fixes

Security policies

Creating exceptions from an “Environment discovery” log

Support reference: 167745PW

Exception rules can now be created in the administration console based on logs generated by the advanced “Environment discovery” protection.

Modifying the volume type in an application ID

Support reference: 167477PW

Whenever the **Volume type** criterion was removed from an identifier and added back to the same identifier, the settings of the criterion could not be modified. This issue has been fixed.

Importing and exporting rule sets

Support reference: 168385PW

Whenever **.cab** files were imported in the panel of shared rule sets, an error message would appear if the files did not contain any shared rules. The message has been improved to state the cause of the error.

Whenever rule sets are exported, the names of the export files now specify whether the sets are shared or private.

Agent logs in the administration console

Searching for agents

Support reference: 167508PW

In the **Agent logs** panel, searches performed via the **Agent** column now make it possible to include all agents, not only those in the list shown in this column.

Special and accented characters in agent group names

Support reference: 167581PW

In the **Agent logs** panel, special and accented characters are now correctly displayed in the **Agent group** column.

Log display in the console

Support reference: 188215CW

When rule-generated logs were configured to never appear on the console, they appeared nonetheless. This setting now works correctly.



Advanced log filters

In the advanced filters of the **Agent logs** panel, the Enter key no longer wrongly adds a new line or automatically confirms the form.

Logs generated by self-protection events

Support reference: 167586PW

In the **Agent logs** panel, the **View rule** button is no longer available for logs generated by self-protection events, since such logs do not match any rules.

User name in incidents

Support reference: 189879CW

In the **Agent logs** panel, the user name is now shown in the **Agent** column of each incident, as was already the case for standard logs.

Managing agent groups

Filtering agents by agent groups

In the **Agents** menu of the administration console, the **Default group** filter in the **Group** field now always shows the agents of the default group after the interface language is changed.

Applying conditional security policies

Support reference: 168192PW

In agent group configuration, conditional policies that use scripts as a condition of application are now applied in the right order.

Maintenance mode disabled

When Maintenance mode is not allowed in the agent group configuration, the button to enable Maintenance mode in the advanced settings of the agent's **Preferences** tab is now grayed out.

Deploying the environment

Timeout after a deployment error

Support reference: 189042CW

When an issue occurs during the deployment of an environment, and the deployment stops, a new deployment can only be attempted 15 minutes later. The timeout was previously set to 30 minutes.



SES Evolution agents

Optimizing performance

Support reference: 187968CW

The impact of the SES Evolution agent on the performance of process launches has been optimized. It allows improving the compatibility with the Xilinx SDK.

Support references: 185692CW and 186425CW

The protection of access to the registry database and the identification of processes have been improved so that they no longer affect the performance of workstations.

Updating the SES Evolution agent

Support reference: 186717CW

Searches for updates from the agent's interface no longer cause an error, and now function correctly.

Deleting logs

Support reference: 167479PW

SES Evolution logs are now effectively deleted from workstations' disks after the number of days indicated in the configuration of the agent group.

Blocked EsUpdate and EsUpdateHost processes

Support reference: 167481PW

The SES Evolution self-protection mechanism now no longer blocks the EsUpdate and EsUpdateHost processes over port 80.

Compatibility with Microsoft Excel

Support reference: 186764CW

Keylogging protection no longer makes Microsoft Excel shut down unexpectedly.

Improved performance when a USB device is plugged into an air-gapped workstation

Support reference: 187720CW

An incompatibility with Windows Defender's real-time protection, which occurs when a USB device is plugged into an air-gapped workstation, would slow down the workstation. This incompatibility has been fixed.

Compatibility with Microsoft PowerPoint

Support reference: 188228CW

SES Evolution no longer shuts down Microsoft PowerPoint unexpectedly when the workstation switches out of hibernation mode.



Agent handlers

Time zone

Support reference: 189338CW

An issue with the time zone on the machine hosting the agent handler could block log processing and log recording in the database. This issue has been fixed.



Version 2.2.1 not published

Version 2.2.1 is not available to the public.



Version 2.2.0 not published

Version 2.2.0 is not available to the public.



Resolved vulnerabilities for SES Evolution 2.1.2

Backend

A high severity vulnerability was fixed. Details on this vulnerability can be found on our website <https://advisories.stormshield.eu/2021-070/>.

Administration console

A medium severity vulnerability was fixed. Details on this vulnerability can be found on our website <https://advisories.stormshield.eu/2021-071/>.

Logs

A low severity vulnerability was fixed. Details on this vulnerability can be found on our website <https://advisories.stormshield.eu/2021-072/>.



SES Evolution 2.1.1 fixes

Installation

You can now launch an update a second time via the Installation Center if it was canceled the previous time.

Support references: SESNG-7486

The Installation Center now correctly verifies the backend component password.

Support references: SESNG-7842

Stormshield default policy

When keylogging protection is enabled, KeePass Password Safe is no longer prevented from automatically entering passwords

Support references: SESNG-7714

Wi-Fi rules that were initially in the *Protection baseline* rule set have been outsourced to an independent rule set that is not included by default in policies. In this way, the software security policy can be kept separate from the hardware component usage policy. In addition, Wi-Fi and general device rules no longer generate incidents systematically.

Support references: SESNG-7865

By adding a new root certificate that Google Chrome uses, the browser can be started again when a user clicks on a hypertext link in an e-mail in Microsoft Outlook.

Support references: SESNG-8105

The SQL Server VSS Writer identification mode has been changed. Now it no longer freezes when it writes information to the Shadow Copies registry.

Support references: SESNG-8399

Microsoft Office applications that write .js extension files no longer raise alarms.

Support references: SESNG-8444

To reduce the occurrence of false positives, some heuristic rules that detect password-stealing malware were removed from the policy, and two Microsoft programs known to access raw volumes were added to the policy.

Rule sets

Links to policies in the panel of a rule set are now kept when the **Update all** action is used.

Support references: SESNG-8335

Protection rules

In file rules or application identifiers, file paths containing errors could previously be entered. These are now verified.

Support references: SESNG-8345



OSSEC rules

Some of the file paths that must be monitored in OSSEC rules prevented the policy from being applied. This issue has been fixed. **Support references: SESNG-8345**

Logs

Rules created when an exception is added from a log are now configured correctly. **Support references: 183722CW**

SES Evolution no longer generates errors when there is a large volume of context logs. **Support references: 167478PW**

SES Evolution agent

When events are exported in the SES Evolution agent interface, a list of technical errors is no longer displayed. **Support references: 184781CW**



SES Evolution 2.1 new features

New protections

Advanced protections

Advanced protections make it possible to protect your pool from malicious operations such as the theft of authentication credentials, malicious use of Windows tools, persistent techniques, etc.

 [Find out more](#)

New built-in policy: Protection of backoffice components

A built-in security policy is now equipped to increase the security of SES Evolution backoffice components. This policy must be applied to agent groups that contain agent handlers, backends and the administration console.

In addition to the security features in the default policy, it includes several modular rule sets, each of which corresponds to a backoffice component. The policy consists of the following rule sets:

- Audits of attack contexts,
- Backend protection (new),
- Agent handler protection (new),
- Administration console protection (new),
- Advanced protections (new),
- Protection baseline.

 [Find out more](#)

Changes to existing policies

The default policy has been enriched with new rule sets that provide advanced protections and protection from theft of sensitive information.

It now consists of the following rule sets:

- Audits of attack contexts,
- Advanced protections (new),
- Data leak prevention (new),
- Protection baseline.

When updating from SES Evolution 2.0.x to version 2.1, refer to the [Recommendations](#) to find out the steps to take with regard to policy updates.

New built-in rule sets

The following rule sets have been added:

Backend protection	Protects the IIS application server (programs, settings, injection, etc.), database and SES Evolution Installation Center.
Agent handler protection	Protects the agent handler (programs, settings, injection, etc.), database and SES Evolution Installation Center.



Administration console protection	Protects the SES Evolution administration console (programs, settings, injection, etc.), database and SES Evolution Installation Center.
Advanced protections	Unlike protections that react to a strong individual event, advanced protections react to a pattern of several weak events, which when combined, represent a threat.
Data leak prevention	Protects some specific applications used frequently in organizations, e.g., web browsers, file transfer tools, vaults, Windows security authorities and remote control tools. This protection mode covers unauthorized access to files, registry locations and keylogging attempts to deter the theft of sensitive assets. Windows security authorities are also protected from interprocess access, which prevents the extraction of Windows passwords. Special attention is given to programs that allow external code to run (e.g., script engines, DLL loaders, etc.), so that their operations will always be blocked. Likewise, programs provided by default with Windows (LOLBIN) that allow indirect access to information, are blocked.
Windows Defender event forwarding	Consolidates in the administration console security alerts of interest that Windows Defender raises on protected workstations in the SES Evolution pool. It is not included in built-in policies, so it must be added manually to your policies.

Changes to existing rule sets

The following rule sets have been modified:

Audits of attack contexts	<ul style="list-style-type: none">• Operations by programs that allow external code to run (e.g., script engines, DLL loaders, etc.) are now always logged, even when they are signed.• The list of certificates that the rule set recognizes has been enriched.• Rule severity levels have been revised so that no rule is below the agent group's default threshold (<i>Notice</i> level being the lowest)• Advanced detection of ARP Spoofing has been added to this rule set to detect Man In The Middle attacks.• Optimization to minimize impact on system performance without compromising audit quality. This will also reduce the possibility of losing logs during intense activity.
Protection baseline	<p>This rule set has been enriched and hardened:</p> <ul style="list-style-type: none">• Settings cannot be changed in safe mode,• BCD (Boot Configuration Data) is now protected,• Applications recognized as hacking tools have been enriched,• Script engines can no longer be run from browsers,• System configuration files (hosts, services and network) are now protected from unwanted changes,• Third-party programs are monitored and not allowed to run from MS Office applications,• Heuristic analysis of malicious data theft programs, based on the name of the accessed file, has been improved• Unsigned services are monitored and prevented from running.



Agent management

Agent groups based on Active Directory criteria

Agents can be automatically assigned to an agent group according to the Active Directory groups or organizational units to which they belong. This feature saves time and lowers the risk of error when creating agent groups.

 [Find out more](#)

Uninstalling agents

You can now prevent the local administrator of a workstation from uninstalling the SES Evolution agent. In this case, the agent can still be uninstalled via a challenge.

 [Find out more](#)

Agent filtering

New filters now make it possible to show the list of agents by criteria such as operating system, status, security policy, etc.

 [Find out more](#)

Dashboard

A new diagram now appears in the dashboard of the administration console and shows the number of agents in the pool for each version of SES Evolution.

 [Find out more](#)



Database

Log retention in the database

The duration of log retention in the log database can be configured, either when SES Evolution is installed, or at any time through the new **System** menu in the administration console. When logs reach the end of their retention period, they will be deleted by a task that runs regularly.

[Find out more](#)

Versions of policies and rule sets

The versions of policies and rule sets are now better managed to optimize storage space in the administration database.

[Find out more](#)

Removable devices

The list of known USB devices (vendor and product) has been updated in the administration console.

Activity monitoring

Windows event monitoring

Windows events of your choice can be forwarded to SES Evolution so that security information about your environment can be displayed.

[Find out more](#)

Logging of user activity

User activity in the SES Evolution administration console is now logged through a full audit of operations performed.

[Find out more](#)

Backoffice component logs

A new menu in the administration console, **System logs**, shows the activity of agent handlers, backend servers and the SES Evolution administration console.

[Find out more](#)

OSSEC analysis engine

OSSEC rules can now be imported into security policies from the administration console. This allows agents to subscribe to text-based logs or Windows events, and report them as SES Evolution logs in the log database or an SIEM.

[Find out more](#)

Exporting to syslog servers

Logs can now be exported to several syslog servers and the export formats IDMEF and CEF have been added to facilitate their integration into your solutions.

[Find out more](#)



Resolved vulnerabilities for SES Evolution 2.1

Agent

Loading DLLs

A vulnerability would occasionally cause some processes on the agent to load DLLs located elsewhere than in the agent's installation folders. This vulnerability has been fixed.

Details on this vulnerability can be found on our website <https://advisories.stormshield.eu>.

Backend

Access to custom scripts

A moderate severity vulnerability was fixed after the SES Evolution backend component was upgraded.

Details on this vulnerability can be found on our website <https://advisories.stormshield.eu>.

Changes to unused scripts

A moderate severity vulnerability was fixed after the SES Evolution backend component was upgraded.

Details on this vulnerability can be found on our website <https://advisories.stormshield.eu>.

Removal of unused scripts

A low severity vulnerability was fixed after the SES Evolution backend component was upgraded.

Details on this vulnerability can be found on our website <https://advisories.stormshield.eu>.

Removal of application identifiers

A moderate severity vulnerability was fixed after the SES Evolution backend component was upgraded.

Details on this vulnerability can be found on our website <https://advisories.stormshield.eu>.

Changes to security policies

A moderate severity vulnerability was fixed after the SES Evolution backend component was upgraded.

Details on this vulnerability can be found on our website <https://advisories.stormshield.eu>.

Duplication of security policies

A moderate severity vulnerability was fixed after the SES Evolution backend component was upgraded.

Details on this vulnerability can be found on our website <https://advisories.stormshield.eu>.



SES Evolution 2.1 bug fixes

Installation

In the Installation Center, *Minimum installation* has been renamed *Demo installation* to indicate that it must not be used in a production environment, only for testing or demos. *Advanced installation* has been renamed *Standard installation*.

Support references: SESNG-6898

The Installation Center no longer shuts down unexpectedly when the SQL user is unknown. A clear message now informs the user of the issue.

Support references: 182618CW

The language of the Installation Center is now the same as the language of the operating system when it is either French, English, Spanish or German. The Installation Center appears in English for operating systems in other languages.

SES Evolution Agent

Support references: 183130CW

In some cases during startup, the SES Evolution agent would wrongly detect an integrity issue, which would then require a restart. This issue has been fixed.

Support references: SESNG-7184

A compatibility issue between the SES Evolution and the CCleaner application has been fixed.

Support references: SESNG-5426

A blue screen (BSOD) would sometimes occur when the host switched to standby mode. This issue has been fixed.

Security rules

Support references: 181886CW

Exception rules can now be created from logs containing UNC paths.

Support references: 182180CW

Rules can now be copied/pasted or cut/pasted within the same rule set.

Support references: SESNG-5365

Process hollowing protection has been improved.

Support references: SESNG-7226

Privilege escalation rules in an audit rule set no longer prevent the evaluation of rules found in the rule sets that follow.

Support references: SESNG-5295

The *Detect only* action is no longer offered in keylogging protection rules. It was made redundant with the *Passive rule* mode.



Support references: SESNG-5370

All file access originating from the network can now be blocked using file access control rules.

Support references: SESNG-6878

A message now appears if you create an identifier with a path that ends in one or several space characters.

Logs

Support references: 182073CW

In the administration console, the attack chart now displays correctly when it contains WiFi logs.

Support references: SESNG-6372

Filters that exclude agent logs did not always function in the administration console. This issue has been fixed.

Support references: 183960CW

After users are deleted, they no longer appear in the list of users when logs are edited.

Device control

Support references: SESNG-5580

Occasionally, the agent would not display an authorization message when a USB device was plugged in, even though the USB device access control rule required it. This issue has been fixed.

Dashboard

Support references: SESNG-5780

When the SES Evolution environment contains several agent handlers, their status is now correctly displayed in the administration console's dashboard.

Agent management

Support references: SESNG-5505

Agent groups can no longer be created with invalid parameters.

Support references: SESNG-6910

The status of stopped agents now displays correctly in the **Agents** page of the administration console.

Support references: SESNG-7391

The Windows 10 21H1 operating system now displays correctly in the **Agents** page of the administration console.



Compatibility with other firewalls

Compatibility with other firewalls has been enhanced.

Support references: SESNG-5309



SES Evolution 2.0.2 fixes

SES Evolution upgrade

New version of policies

When SES Evolution is updated, Stormshield security policies are now updated as well.

Open administration console

The **Force update** button can now be used in the Installation Center to continue with an update even when an administration console is still open.

Error while updating the administration console

Updating the administration console no longer causes a recurring error in the logs of the backend component. The log is now generated at one go.

Updating the SES Evolution agent

After the SES Evolution agent was updated, it would occasionally prevent some processes from launching. This issue has been fixed.

Security Policies

Importing and exporting rule sets

Rule sets can now be exported and imported again into another SES Evolution environment in the same version.

Application identifiers

Using recursive identifiers and certificates together within the same security rule to identify an application would sometimes cause a blue screen. This issue has been fixed.

SES Evolution default policy

The default policy now includes compatibility with the Hardening mode in Panda Adaptive Defense 360. SES Evolution hides process hollowing operations when Panda causes them for legitimate reasons.

The audit rule set in the default policy was modified to restrict logs that are not relevant to security administrators. This reduces the number of logs displayed and the amount of system CPU that SES Evolution uses.

SES Evolution Agent

Support references: 178084CW - 180244CW

Under certain conditions, SES Evolution agents would send status information that would be misinterpreted by the agent handler. In such cases, the information displayed on the **Agents** panel of the administration console could be incorrect. Various other issues could also occur, such as the administrator being unable to respond to challenges. This issue has been fixed.

Agents waiting to be restarted after features are changed are now displayed correctly in the dashboard of the administration console.



Removable devices

Support references: 180798CW - 164622PW

Using *FTDI Chip* products no longer causes a blue screen. Overall compatibility with devices has been enhanced.



Resolved vulnerabilities for SES Evolution 2.0.1

Protection against denial of service attacks added

Protection against DDoS attacks was added to the API that registers new agent handlers in the Backend. Now only one agent handler can be registered every 15 seconds.

Value in the registry deleted

A value relating to the security of challenges was unnecessarily present in the registry. This vulnerability was fixed by deleting this value.



SES Evolution 2.0.1 fixes

Installing SES Evolution

Password fields

In the Installation Center, the password and confirm password fields are now always correctly verified.

License validity

In the Installation Center, the format and validity of the license are verified as soon as the license file is selected, instead of at the end of the installation.

Security Policies

Support reference: 177214CW

Network access

Some types of network access were not filtered by application protections because they were initiated by the system. They can now be blocked. This option makes it possible to block remote access to shared folders located on workstations that are protected by the SES Evolution agent.

If you upgrade SES Evolution to version 2.0.1, the default policy is not updated. You can download the corresponding rule set from your dedicated [MyStormshield](#) area to add network access permissions for system processes. For more information, refer to the Stormshield [Knowledge base](#).

Network IDs

The **Invert identifier scope** option is now correctly saved in the network ID editing window.

Audit rules on drivers

Specific behavior in the *Driver loading* and *Driver integrity* protection rules is now correctly applied. These rules no longer generate unjustified logs for allowed drivers.



Logs

Searching in agent logs

In the administration console, the maximum duration of an agent log search has been increased from 30 seconds to 15 minutes. A message now appears when the search exceeds this duration.

Displaying incidents

When an incident is opened, only alert logs are now displayed, up to a maximum of 1000 logs. The remaining logs are loaded when the attack chart is consulted, up to a maximum of 100000 logs. This makes it possible to build an attack chart with comprehensive logs.

SES Evolution Agent

Lengthy logs

Lengthy logs no longer cause the graphical interface of the SES Evolution agent to unexpectedly shut down.

Self-protection rules

Self-protection rules on some registry keys of SES Evolution agents were not correctly applied. This issue has been fixed.

Display

Windows 10 agents

The **Agents** panel in the administration console now displays the correct version of the operating system for Windows 10 agents.



Summary of features

Version 2.0 of SES Evolution offers the following features.

SES Evolution 2.0 features

Protection	
Memory overflow	Protects your pool from intrusion attempts and vulnerability exploitation.
Process hollowing	
Security token theft	
File system bypass	
Keylogging	
File access control	Controls all system resources and access to them. Allows applications to make changes, access these resources or blocks them. You can also simply monitor them.
Registry base access control	
Memory access control	
Execution control	
Driver loading detection	Detects rootkits that attempt to load or change drivers in the kernel.
Driver alteration detection	
Application firewall	Controls incoming and outgoing network communications for each application.
Wi-Fi access point control	Manages allowed Wi-Fi networks and prevents the Wi-Fi-LAN bridge from being set up.
Floppy disk or CD/DVD drive control, serial ports	Controls devices allowed in your pool through fully customizable rules.
Bluetooth device control	
USB device control	
USB decontamination air gap	Controls the USB keys and hard disks in your pool, manages trusted devices and blocks devices that have not been validated.
Configuration	
Management via agent groups	Organizes your pool according to your requirements through a simple but powerful system of agent groups.
Configuration deployment	Deploys new configurations in all agents with a single click in the administration console.
Stormshield security policy	Protects your pool with a default policy that covers common threats and adds custom security rules to fully adapt the policy to your environment.
Context-based security policies	Adapts security to agents' environment so that they apply different policies based on their location.
Policy management through rule sets	Pool security rules in your policies and manage exceptions easily.



Scheduled tasks	Runs commands on agents by configuring scripts from the administration console.
Agent modularity	Manages features installed on each agent from the administration console: uninstall unused features, delete incompatible versions and reduce the attack surface.
Challenges	Allows some operations to be performed securely through a question/response system.
Simultaneously connected administrators	Organizes your administrators by role to manage simultaneous access to various resources on the administration console.

Activity monitoring

Dashboard	See the status of your pool in a glimpse with a simple dashboard.
Log tracking	Views events that agents raise, filtering them by priority, type, group, etc.
Attack analysis	Follows incidents and analyzes attacks in a dedicated panel that illustrates steps in charts and provides additional information to better understand each attack.
Agent monitoring	Tracks the pool's agents in real time, checks their status and assigns them to groups
Syslog server export	Exports all events in your SIEM system to include them in your other sources of security information (firewall, antivirus, etc.).



Contact

To contact our Stormshield Technical Assistance Center (TAC):

- <https://mystormshield.eu/>
All requests to technical support must be submitted through the incident manager in the private-access area https://mystormshield.eu, under Technical support > Manage cases.
- +33 (0) 9 69 329 129
In order for us to provide high-quality service, you are advised to use this communication method only to follow up on incidents that have been created earlier on https://mystormshield.eu.



STORMSHIELD

All images in this document are for representational purposes only, actual products may differ.

Copyright © Stormshield 2023. All rights reserved. All other company and product names contained in this document are trademarks or registered trademarks of their respective companies.